AMENDMENTS TO THE CLAIMS

The listing of claims below replaces all prior versions of claims in the application.

1. (Currently Amended) Method for automatically identifying an access right to protected areas in a first network using a unique connection identifier of a second network, ~~with~~ comprising the following procedural steps:

[[-]] dynamic or static assignment of a unique identifier of the first network for a terminal, during or prior to the latter's connection to the first network by means of the second network;

[[-]] storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit;

[[-]] ~~the~~ a provider of the protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area;

[[-]] ~~authentication~~ authenticating the unique connection identifier of the second network and/or ~~communication exclusively of~~ communicating the unique connection identifier of the second network to the provider of the protected area by means of the authentication unit; and

[[-]] checking whether an access right for the protected area exists for the unique connection identifier of the second network.

2. (Previously Presented) Method in accordance with claim 1, wherein the combination stored in the current authentication unit contains further data in addition.

3. (Currently Amended) Method in accordance with claim 2, ~~characterized in that~~ wherein the additional data has at least one of the following:

the dial-in number into the first network, a user name (login) and a password.

4. (Previously Presented) Method in accordance with claim 1, wherein the authentication unit is only run temporarily.

5. (Previously Presented) Method in accordance with claim 4, wherein the combination of data is deleted from the authentication unit as soon as the terminal ends its connection with one of the two networks.

6. (Previously Presented) Method in accordance with claim 1, wherein the unique identifier of the second network is a call-up number.

7. (Previously Presented) Method in accordance with claim 1, wherein the protected area includes the provision of an online individual connection identification.

8. (Currently Amended) Method in accordance with claim 7, wherein [[a]] an individual connection identification takes place automatically for the unique connection identifier of the second network.

9. (Currently Amended) Method in accordance with claim 7, wherein, before release of [[a]] an individual connection identification, a further entry on the terminal is necessary ~~in addition~~.

10. (Previously Presented) Method in accordance with claim 9, wherein the further entry includes the entry of an invoice number and/or a customer number and/or a PIN.

11. (Currently Amended) Method in accordance with claim 1, wherein only ~~authorised~~authorized services have access to the authentication unit.

12. (Previously Presented) Method in accordance with claim 1, wherein the protected area includes at least one of the following services:

provision of contents, electronic trade (e-commerce), payment or settlement services and authorized services.

13. (Previously Presented) Method in accordance with claim 12, wherein with a payment service, the costs arising are automatically invoiced by means of the unique connection identifier of the second network.

14. (Currently Amended) Method in accordance with claim 1, ~~characterized in that~~ wherein further data are automatically called up from the terminal and/or further procedural steps are initiated in the protected area using the unique connection identifier of the second network.

15. (Currently Amended) Method in accordance with claim 1, wherein further ~~personalisation~~ personalization of the terminal takes place by entering a PIN.

16. (Currently Amended) Method for providing data for automatic identification of access rights to protected areas in networks, ~~with~~ comprising the following procedural steps:

[[-]] provision of at least one unique identifier respectively from at least two different networks while a connection to both networks exists, whereby the connection to one of the networks happens by means of the other network;

[[-]] storage of a combination of ~~the different~~ the unique identifiers in an authentication unit;

[[-]] ~~authentication~~ authenticating and/or ~~issue exclusively~~ issuing of one of the unique identifiers when a corresponding enquiry is made regarding ~~the other~~ an other of the unique identifiers; and

[[-]] deletion of ~~the~~ data from the authentication unit as soon as a connection with at least one of the two networks has ended.

17. (Previously Presented) Method in accordance with claim 16, wherein at least one of the identifiers is an IP number and/or a unique connection identifier of a terminal.

18. (Currently Amended) Method in accordance with claim 16, wherein it is checked whether the enquiry originates from an ~~authorised~~authorized place or from an ~~authorised~~authorized service.

19. (Previously Presented) Method in accordance with claim 16, wherein the combination stored in the current authentication unit contains further information in addition.

20. (Previously Presented) Method in accordance with claim 19, wherein the additional data have at least one of the following: a dial-in number into one of the networks, a user name (login) and a password.

21. (Previously Presented) Method in accordance with claim 16, wherein a call-up number block or a target number block is identified by means of the authentication unit.

22. (Previously Presented) Method in accordance with claim 1 or 16, wherein the first and second networks are based on different protocols.

23. (Previously Presented) Method in accordance with claim 1 or 16, wherein the first network is the internet, and the second network is a telephone network.